

IOWA STATE UNIVERSITY
OF SCIENCE AND TECHNOLOGY

February 1, 1994

DOCKET FILE COPY ORIGINAL

Telecommunications
371 Durham Center
Ames, Iowa 50011
515 294-8585
FAX 515 294-1000

RECEIVED

FEB - 8 1994

FCC MAIL ROOM

Mr. William F. Canton
Acting Secretary
Federal Communications Commission
1919 M Street NW
Washington, DC 20554

RE: CC Docket No. 93-292

Dear Mr. Canton:

I am a telecommunications professional who is responsible for my university's telecommunication systems, and I am painfully aware that although I may reduce the risk, no matter how many steps I take to secure my systems, I am still vulnerable to toll fraud. That is why I am so encouraged by the proposed rule making.

PBX owners should not be responsible for 100% of toll fraud if we are not controlling 100% of our destiny. This destiny is ultimately controlled by not only our implementation and proper use of PBX security features, but by the information, equipment, and services provided by IXC's, LEC's, and CPE vendors. The legal obligations of the IXC's, LEC's, and CPE vendors should provide the proper incentive to reduce and eliminate all toll fraud.

Current programs offered by some IXC's (Sprint Guard™, MCI Detect™, and AT&T Netprotect™) and insurance companies are too expensive. Monitoring and proper notification by the IXC's must be a part of the basic interexchange service offerings. This should eliminate cases of toll fraud greater than 24 hours.

LEC's must also provide monitoring and proper notification as a part of their basic service offerings. Local lines are as vulnerable to toll fraud. As the line between IXC and LEC becomes fuzzier, monitoring and proper notification by all carriers will be even more applicable.

CPE vendors need to provide telecommunications security as a cost of doing business instead of an opportunity to sell additional products and services. CPE vendors should be required to provide warnings about the risks of toll fraud, as it specifically relates to their equipment and provide solutions to reduce the risk of toll fraud. All CPE should be delivered without standard default passwords, which are well known to the criminal community. All login IDs, including those used by the vendor, should be disclosed at the time of purchase and at installation. All customer passwords should be changed or created at installation and the customer should receive written assurance that all vendor passwords will meet minimum requirements regarding length, change schedule, and alpha numeric format. CPE vendors should be encouraged to offer security-related hardware and software in the price of their systems.

No. of Copies rec'd
List ABCDE

Aug.

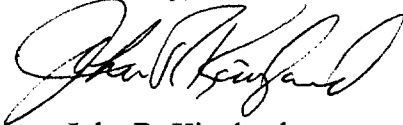
The provisions outlined in the NPRM are fair and equitable. Shared liability will require clearly defining the responsibilities of the:

- CPE owner to secure their equipment
- CPE vendors to warn customers of the specific toll fraud risks associated with their equipment
- IXC's and LEC's to offer detection, notification, prevention, and education offerings and services

If toll fraud occurs due to the negligence of one or more parties then the financial loss should be equitably distributed among those negligent parties. If there is no proven negligence, the financial loss should be equitably distributed among CPE owner, and all CPE vendor(s), LEC(s), and IXC(s) involved.

Toll fraud is a financially devastating problem that affects the entire telecommunications industry including users, vendors, and carriers. I am sure that if we all work together we can and will make a positive impact on this problem.

Sincerely,

A handwritten signature in black ink, appearing to read "John R. Kingland", written in a cursive style.

John R. Kingland
Director

CPC International Inc.
P.O. Box 8000, International Plaza
Englewood Cliffs, NJ 07632-9976

January 28, 1994

CPC
International

SUBJECT: FCC DOCKET NO. 93-292

Mr. William F. Caton
Acting Secretary
Federal Communications Commission
Common Carrier Bureau
1919 N. Street N.W.
Washington, D.C. 20554

RECEIVED
FEB 8 1994
FCC - MAIL ROOM

Dear Mr. Caton:

CPC International is a Fortune 100 company engaged in the food industry with over one hundred offices and production facilities throughout the United States. Various types of telephone fraud have plagued this corporation for a number of years. Since the FCC is addressing telephone fraud in the subject docket, I feel compelled to comment on behalf of CPC International.

For years, we have maintained a position that PBX and other telecommunications equipment manufacturers and distributors should bear a percentage of the financial responsibility for their customers risk of toll fraud. Since PBX manufacturers and voice processing equipment manufacturers are, or should be, intimately aware of the engineering intricacies of their systems, they and their distributors should be responsible for disclosing all toll fraud risks inherent in their systems to the customer prior to installation. If, under contractual terms, a customer accepts such risks, the manufacturer or distributor should not bear liability. Manufacturers would be prudent to establish system default parameters which limit a customers exposure to toll fraud unless otherwise directed by the customer, in writing.

CPC International also believes the carriers should bear a percentage of the financial responsibility incurred by customers as a result of toll fraud because of their ability to capture and secure toll call information, real time. If the carriers were made to bear a portion of the financial burden incurred with toll fraud, they may be more responsible notifying a customer about abnormal traffic patterns.

In addition, we are of the opinion that the minimum dollar threshold of exposure to toll fraud before the Secret Service will investigate a claim must be reevaluated because of the proliferation of the toll fraud industry. A few years ago toll fraud was a problem, today it is big business. The only deterrent for conducting this type of business may be fear of prosecution and incarceration.

CPC International appreciates this opportunity to provide the FCC these comments having been a victim of toll and other telecommunications fraud.

Sincerely,

Kathleen N. Spola

Kathleen N. Spola
Manager, Telecommunications

No. of Copies rec'd
List ABCDE

4 copies

Society

Society Corporation
127 Public Square
Cleveland, Ohio 44114-1306

DOCKET FILE COPY ORIGINAL

RECEIVED

FEB 8 1994

FCC MAIL ROOM

February 4, 1994

VIA AIRBORNE MAIL

Office of the Secretary
Federal Communications Commission
Washington, DC. 20554

Re: CC Docket No. 93-292; FCC 93-496 Notice of
Rulemaking Concerning Toll Fraud

Dear Sir or Madam:

On behalf of Society Corporation ("Society"), Cleveland, Ohio, I submit this letter as our comment to the Federal Communication Commission ("FCC") Policies and Rulemaking Concerning Toll Fraud. Society is a bank holding company with assets in excess of \$25 billion, with banks and other financial service subsidiaries doing business in Ohio, Michigan, Indiana and Florida.

We are in agreement with the FCC, that an overall review of this issue is necessary to establish safeguards in the prevention of toll fraud. We greatly appreciate having the opportunity to comment on the proposed rule, and would offer the following observations.

We believe that any program developed to eliminate fraud must be applied in a comprehensive manner, and administered by the FCC. The inter exchange carriers ("IXC") are in the best position to implement broad coverage, and the FCC has the capability to ensure a standard level of service quality. By requiring the IXC's to have toll fraud monitoring as part of their basic service offerings, the FCC would be taking a large step toward the prevention of toll fraud.

The proposed rules will place new burdens upon customer premise equipment ("CPE") vendors, requiring warnings explaining the risks of using their equipment. It is our belief that warnings in and of themselves are helpful, but insufficient to prevent toll fraud. We feel that several other measures should be implemented. Examples of such measures are as follows:

024

- **Mandate that all systems provide an access audit trail, reflecting a record of the type of changes made and the access ID used.**
- **Have toll fraud protection parameters set as the factory default. Examples of such parameters are those that require voice mail calls to be transferred to stations only, and those that would limit the number of invalid password attempts. In addition, private branch exchange ("PBX") equipment should be delivered without standard default passwords, and designed so that passwords expire at regular intervals.**
- **Design systems so that the features most subject to fraud, such as remote access, would have to be specifically ordered by the customer.**
- **Require that each PBX vendor provide a free consultative service to its customers to enable them to deal more effectively with toll fraud issues.**

Thank you for providing Society with an opportunity to comment on the proposed rulemaking concerning toll fraud prevention. We would be happy to discuss our comments with you or your staff at further length. If you have any questions or comments, please feel free to call Ms. Mickey Bauer, Corporate Information Security Analyst, at (216) 689-8456.

Very truly yours,



**Neil P. Allegretto
Senior Vice President
Society Management Company**